



Implementing, Monitoring, and Troubleshooting Security Accounts and Policies

Terms you'll need to understand:

- ✓ Local users and groups
- ✓ Workgroup
- ✓ Domain
- ✓ Domain users and groups
- ✓ Active Directory
- ✓ Organizational unit (OU)
- ✓ Policy
- ✓ Privilege or user right

Techniques you'll need to master:

- ✓ Creating local users and groups
- ✓ Creating domain users and groups
- ✓ Managing user and group properties
- ✓ Dealing with changes in your user population, such as renaming and copying accounts
- ✓ Securing a system
- ✓ Creating a local and group policy

Networks' *raison d'être*—their reason for being—is to allow users to access resources such as files, printers, and applications on computers other than the ones at which they are sitting. In an ideal world, we would trust every user with every file we create, and all we'd have to do is connect our computers to a network and share it all. Unfortunately, we don't trust every user with every file we create. In the real world, certain users need access to resources that others should be restricted from accessing. Therefore, we need user accounts to identify and authenticate users when they attempt to access resources. But imagine trying to define who can access a resource and at what level if you had to worry about each individual user! Using groups significantly eases the process of defining resource access; you can assign permissions and privileges to groups and thereby define access for their members, and groups may contain one, dozens, hundreds, or thousands of users.

This chapter highlights critical skills and concepts related to user, group, and computer accounts, and the process of creating security configurations and policies for a Windows 2000 Professional system.

User and Group Accounts

Windows 2000 Professional creates several default local users and groups when you first install the operating system. When you join a Windows 2000 Professional computer to a Windows domain (within a Windows NT Server, Windows 2000 Server, or a Windows Server 2003 network), several additional user and group accounts come into play from the domain. Understanding the functions of the various local users and groups and knowing the differences between local user and group accounts and domain user and group accounts is key to being an effective network administrator and important for success on the Windows 2000 Professional certification exam.

Local and Domain Accounts

User and group accounts are stored in one of two locations: the *local security database* or the domain's *Active Directory* database. When an account is created in the local security database, that account is called a *local user* or *local group*.

Each Windows 2000 Professional system has two default local user accounts—Administrator and Guest (which is disabled by default)—and several built-in group accounts, which are discussed shortly. Local user and group accounts provide privileges and permissions to resources of the system

on which they are defined. For example, the Users group has the privilege to log on locally. As you create local user accounts, they are members of the Users group by default; those users are then given the privilege to log on to that system.

Local user and group accounts cannot be given privileges or permissions to resources on any other system because the security database of the system where they are created is truly local: No other system can “see” it. If a user has logged on to a computer by using a local account, the only way that user can gain access to resources of a remote system is through an account for that user on the remote system. That account must be given privileges and permissions or must be placed into appropriate groups on the remote system. When a duplicate or redundant account is created with the same username and password on the remote system as on the local system, the user “seamlessly” accesses resources on the remote system; such users cannot tell that the remote system is authenticating them. However, if the username or password on the remote system is different from that on the local system, the user is prompted with an authentication dialog box when he or she first attempts to connect to the remote system.

Two or more systems that use only their own local accounts being on a network creates what is called a *workgroup*, a kind of peer-to-peer network. You can imagine how difficult managing redundant accounts for a single user on two different systems might become. If a user changes his or her password on one machine, he or she must remember to change it on the other; otherwise, the user is prompted for authentication at each connection. Such challenges would become multiplied many times over in a large workgroup with multiple users and multiple machines.

Thus, networks of any size turn to a *domain* model, in which one or more servers, called *domain controllers*, maintain a centralized database of users and groups. Security accounts in a domain are stored in the domain’s Active Directory database. When a user is created in a domain, that single user account can be given privileges and permissions to resources and systems throughout the domain and in other domains within the enterprise’s Active Directory database. Active Directory is covered in more detail in the “Understanding Active Directory” section later in this chapter.



Domain user and group accounts are stored within the Active Directory database for Windows 2000 Server and Windows Server 2003 domains only. The user and group domain accounts for Windows NT Server and Windows NT Server 4.0 domains are stored within the legacy Security Accounts Manager (SAM) database, which is a less robust user and group directory than Active Directory.



In a domain, it is unusual (and not a best practice) to create or use local user accounts. Most computers that are members of a domain have only the local Administrator and Guest user accounts in their security databases.

Managing Local User and Group Accounts

The Local Users and Groups snap-in allows you to manage—surprise!—local users and groups. You can get to the snap-in by choosing Start, Settings, Control Panel, Administrative Tools, Computer Management and then by expanding the tree pane of the Computer Management console until you see snap-in. In this snap-in, you can create, modify, duplicate, and delete users (in the Users folder) and groups (in the Groups folder).

Using Built-in User and Group Accounts

As mentioned earlier in this chapter, there are two built-in user accounts: Administrator and Guest. The Administrator account

- Cannot be disabled, locked out, or deleted.
- Cannot be removed from the Administrators group.
- Has, through its membership in the Administrators group, all privileges required to perform system administration duties.
- Can be renamed.

The Guest account

- Is disabled by default. Only a member of the Administrators group can enable the account. If the Guest account is enabled, it should be given a password, and User Cannot Change Password should be set if multiple users will log on with the account.
- Cannot be deleted.
- Can be locked out.
- Can be renamed.
- Does not save user preferences or settings.

Built-in local groups have assigned to them specific privileges (also called *user rights*) that allow them to perform specific sets of tasks on a system. The following are the default local group accounts on a Windows 2000 Professional system:

- *Administrators*—Members of this group have all built-in system privileges assigned. They can create and modify user and group accounts, manage security policies, create printers, and manage permissions to resources on the system. The local Administrator account is the default member and cannot be removed. Other accounts can be added and removed. When a system joins a domain, the Domain Admins group is added, but it can be removed.
- *Backup Operators*—Members of this group can back up and restore files and folders, regardless of security permissions assigned to those resources. They can log on and shut down a system but cannot change security settings.
- *Power Users*—Members of this group can share resources and create user and group accounts. They cannot modify user accounts they did not create, nor can they modify the Administrators or Backup Operators groups. Members of the Power Users group cannot take ownership of files, back up or restore directories, load or unload device drivers, or manage the security and auditing logs. Members of the Power Users group can run all Windows 2000-compatible applications as well as legacy applications, some of which members of the Users group cannot execute.



If you want certain users to have broad system administration capabilities but do not want them to be able to access all system resources, you should consider putting them in the Backup Operators and Power Users groups rather than in the Administrators group.

- *Users*—Members of this group can log on to a system, shut down a system, use local and network printers, create local groups, and manage the groups they create. They cannot create local printers or share folders. Some older (legacy) applications do not run for members of the Users group because security settings are tighter for the Users group in Windows 2000 than in Windows NT 4. By default, all local user accounts you create are added to the Users group. In addition, when a system joins a domain, the Domain Users group is made a member of that system's local Users group.
- *Guests*—Members of this group have limited privileges but can log on to a system and shut it down. Members of the Guests group cannot make permanent changes to their desktops or profiles. By default, the built-in local Guest account is a member of this group. When a system joins a domain, the Domain Guests group is added to the local Guests group.

- *Replicator*—This group is used to support file replication services in a domain.

A Windows 2000 Professional system also has built-in *system* groups, which you do not see in the user interface while managing other group accounts. Membership of system groups changes based on how the computer is being accessed or utilized, not based on who is accessing the computer. Built-in system groups are also referred to as special identity groups and include the following:

- *Everyone*—This group includes all users who access the computer, including the Guest account.
- *Authenticated Users*—This group includes all users who have valid user accounts in the local security database or (in the case of domain members) in Active Directory's directory services. You should use the Authenticated Users group rather than the Everyone group to assign privileges and group permissions because doing so prevents anonymous access to resources.
- *Creator Owner*—This group contains the user account that created or took ownership of a resource. If the user is a member of the Administrators group, the Creator Owner group is the owner of the resource.
- *Network*—This group contains any user who currently has a connection from a remote system.
- *Interactive*—This group contains the user account for the user who is logged on to the system locally.
- *System*—This group includes any operating system services that are configured to run within the security context of the operating system itself.
- *Terminal Server User*—This group includes all users who are currently connected to the computer via a remote desktop (that is, terminal services client) connection.
- *Anonymous Logon*—This group includes any user account that Windows 2000 has not authenticated.
- *Dial-up*—This group contains all users that currently use dial-up connections.

Creating Local User and Group Accounts

To create a local user or group account, you right-click the appropriate folder (Users or Groups) and choose New User (or New Group), enter the appropriate attributes, and then click Create.

The following guidelines apply to user account names:

- They must be unique.
- They are recognized only up to the twentieth character, although the name itself can be longer.
- They cannot contain the following characters: " / \ [] ; : , = + * ? < >.
- They are not case sensitive, although the user account's name property displays the case as entered.

You should determine a policy for accommodating users who have the same name. For example, you can add a number after the username (for example, JohnD1, JohnD2). Some organizations also identify certain types of users by their usernames (for example, JohnDoe-Temp for a temporary employee).

The following guidelines apply to user account passwords:

- They are recommended.
- They are case sensitive.
- They can contain up to 127 characters, although down-level operating systems such as Windows NT 4 and Windows 9x support only 14-character passwords.
- They should be a minimum of 7 to 8 characters.
- They should be difficult to guess and, preferably, should mix uppercase and lowercase letters, numerals, and nonalphanumeric characters (other than those listed previously as being prohibited).
- They can be set by the administrator (who can then determine whether users must, can, or cannot change their passwords) or the user (if the administrator has not specified otherwise).

From the Local Users and Groups node of the Computer Management console, or from the Active Directory Users and Computers console on a domain controller, you can select User Must Change Password at Next Logon to ensure that the user is the only one who knows the account's password. You can select User Cannot Change Password when more than one person (such as the Guest user account) uses the account.



The User Cannot Change Password option is not available when User Must Change Password at Next Logon is selected.

The Password Never Expires option is helpful when a program or a service uses an account. To avoid having to reconfigure the service with a new password, you can simply set the service's account to retain its password indefinitely.

Configuring Account Properties

The information you can specify when creating an account is limited in Windows 2000. Therefore, after you create an account, you often need to go to the account's properties sheet, which you can access by right-clicking the account and choosing Properties. Figure 3.1 shows the properties sheets of two accounts.

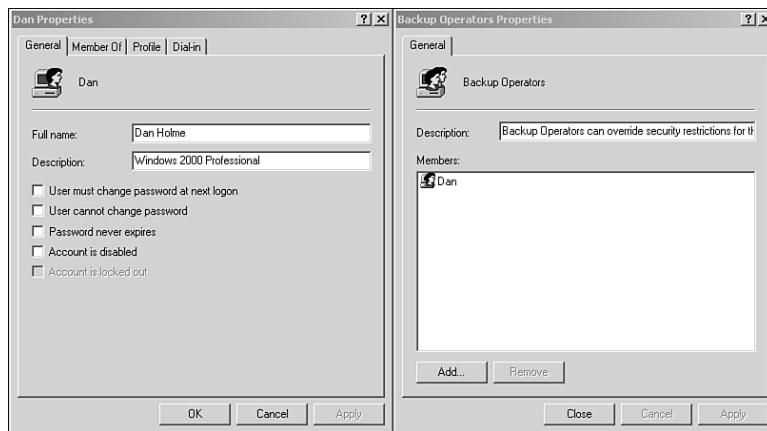


Figure 3.1 The properties sheets of the Dan user account and the Backup Operators group account.

Managing Local Group Membership

To manage the membership of a local group, you right-click the group and choose Properties. To remove a member, you select the account and click Remove. To add a member, you click Add and select or enter the name of the account.

In a workgroup, local groups can contain only accounts defined in the same machine's local security database. When a system belongs to a domain, its local groups can also include domain accounts, including user accounts,

universal groups, and global groups from the enterprise's Active Directory database, as well as domain local groups from within the system's domain.



Universal groups and domain local groups can be added as members only when the domain is in native mode, meaning that it contains only Windows 2000 domain controllers and no legacy (that is, Windows NT 4.0) backup domain controllers.

Renaming Accounts

To rename an account, you right-click the account and choose Rename. Then you type the new name and press Enter. Each user and group account is represented in the local security database by a long, unique string called a *security identifier* (SID), which is generated when the account is created. The SID is what is actually assigned permissions and privileges. The user or group name is just a user-friendly "face" on that process. Therefore, when you rename an account, the account's SID remains the same, so the account retains all its group memberships, permissions, and privileges.

Two situations mandate renaming an account. The first occurs when one user stops using a system and a new user requires the same access as the first. Rather than create a new local user account for the new user, you can simply rename the old user account. The account's SID remains the same, so its group memberships, privileges, and permissions are retained. You should also specify a new password in the account's properties sheet and select the User Must Change Password at Next Logon option.



The easiest way to "replace" a user is to rename the account. Therefore, when one user leaves and another requires the same group memberships, rights, and resource access permissions as the first, you can simply rename the former user's account. You should not forget to reset the account's password because the new user won't otherwise know the old user's password.

The second situation that warrants renaming a user account is the security practice of renaming the built-in Administrator and Guest accounts. You cannot delete these accounts, nor can you disable or remove the Administrator account from the Local Administrators group, so renaming the accounts is a recommended practice for hindering malicious access to a system.

Disabling or Enabling User Accounts

To disable or enable a user account, you open its properties sheet and select or clear the Account Is Disabled check box. If an account is disabled, a user

cannot log on to the system by using that account. The Administrator account cannot be disabled, and only administrators can enable the Guest account.

Deleting Accounts

You can delete a local user or group account (but not built-in accounts such as Administrator, Guest, or Backup Operators) by right-clicking the account and choosing Delete. When you delete a group, you delete the group account only, not the accounts of its members. A group is a membership list, not a container.



NOTE

When you delete an account, you are deleting its SID. Therefore, if you delete an account by accident and then re-create the account, even with the same name, the account does not have the same permissions, privileges, or group memberships as before—you have to regenerate them. For that reason, and to facilitate auditing, it is recommended that you disable, not delete, any user who leaves an organization.

Using the Users and Passwords Applet

A different tool for administering local user accounts is the Users and Passwords applet in the Control Panel. This utility allows you to create and remove user accounts as well as specify group membership for those users. The Users and Passwords applet is wizard driven and is useful for novice administrators and home users. You double-click the Users and Passwords icon in the Control Panel to run this utility. To launch the Local Users and Groups snap-in from the Users and Passwords applet, you click the Advanced tab and then click the Advanced button (in the Advanced User Management section).



NOTE

The Users and Passwords applet provides an opportunity to override the logon requirement for a system. This feature is discussed later in this chapter, in the “Authentication” section.

Managing Domain User Accounts

You manage domain user accounts with the Active Directory Users and Computers snap-in. To access it, you choose Start, Settings, Control Panel, Administrative Tools, Active Directory Users and Computers. Note that unlike in Windows NT 4, in Windows 2000 all domain controllers can make changes to the Active Directory database. When you open the Active Directory Users and Computers snap-in, you connect to an available domain controller. If you want to specify which domain controller or which domain you want to connect to, you right-click the Active Directory Users and

Computers node and choose Connect to Domain or Connect to Domain Controller.

Unlike the local security database, which is a flat list of users and groups, Active Directory has containers such as domains and organizational units (OUs), which collect database objects such as users that are administered similarly to one another. *OUs* are simply containers that allow administrators to logically group Active Directory objects, such as users, groups, and computers. All the objects that are contained within an OU can be administered together. Administration tasks may also be delegated to other administrators for each OU. Therefore, when you manage domain user accounts in Windows 2000, you need to start in the container or OU where the objects reside that you want to work with.

Creating Domain User Accounts

You create a domain user account by right-clicking the OU or container in which you want the user account and then choosing New User. A wizard prompts you for basic account properties, including the following:

- First name
- Initials
- Last name
- Full name (by default, the combination of the first name and last name)
- User logon name and user principal name (UPN) suffix
- User logon name (pre-Windows 2000)
- Password and confirmed password

Windows 2000 user accounts have two logon names. The UPN is used for logon to a Windows 2000 system and consists of a logon name followed by the @ symbol and a suffix, which by default is the Domain Name System (DNS) name of the domain. Each user must have a unique UPN in the domain. The pre-Windows 2000 logon name is used for logging on to pre-Windows 2000 systems such as Windows NT 4, and Windows 95, 98, and Me. Each user's pre-Windows 2000 logon name must be unique in the domain and by default is the same as the logon name portion of the UPN.

Modifying User Account Properties

After an account is created, Active Directory provides dozens of attributes to further define that user. You can right-click a user and choose Properties to open a tabbed dialog box full of attributes that can be defined for that user.

The only properties you can specify when creating the user are those on the Account tab. You must set the remainder of the properties after the account has been instantiated.

Copying User Accounts

A user object in Active Directory may have numerous attributes defined, including work location, group membership, and superiors within the organization. Often, a new user object shares many of its attributes with one or more other user objects. In that case, it is faster to copy an existing user object than to create a new object and define each and every property for the object. To copy a user, you right-click the object and choose Copy. You are asked to enter some of the basic account properties, such as name and password.



You can copy a user only with domain user accounts, not with local user accounts.

Creating Template User Accounts

When you expect to create multiple user objects with highly similar properties, you can create a “template” account that, when copied, initiates the new accounts with its defined attributes. The only trick to working with templates is to disable the template account. Then, when you copy the account to create a new user with predefined attributes, you need to make sure to enable the new account.



When you copy a user account—whether it's a “real” user account or a template—the new copy belongs to all the same groups as the original and therefore has the same resource access that is assigned to the groups of the original account. However, the new copy does *not* have access to resources for which permissions are assigned directly to the original user account.

Disabling and Deleting User Accounts

The process for disabling and deleting domain user accounts is the same as for local user accounts, except that you use the Active Directory Users and Computers snap-in to perform the tasks. The check box for disabling an account is on the user's Account properties sheet.

Adding Domain User Accounts to Local Groups

In Windows 2000 you can add a user to a group with either the group's Members properties sheet or the user's Member Of properties sheet, except

when adding *domain* user accounts to *local* groups, in which case you must use the group's Members properties sheet. A domain user's Member Of properties sheet displays only memberships in global, domain, local, and universal groups.

Authentication

When a user wants to access resources on a machine, that user's identity must first be verified through a process called *authentication*. For example, when a user logs on, the security subsystem evaluates the user's username and password. If there is a match, the user is authenticated. The process of logging on to a machine where you are physically sitting is called *interactive logon*. Authentication also happens when you access resources on a remote system. For example, when you open a shared folder on a server, you are being authenticated, but the process is called *remote* or *network logon* because you are not physically at the server.

The Security Dialog Box

The *security dialog box* allows for interactive logon to a Windows 2000 system. You can access the Security dialog box shortly after a system has started, and at any time after logon, by pressing Ctrl+Alt+Delete. If you are not currently logged on, you can enter a username and password. If the system belongs to a domain, you need to be certain that the domain in which your account exists is authenticating you. You can either select the domain from the drop-down list or enter your UPN. The UPN is an attribute of an Active Directory user object and, by default, has the form *username@dnsdomain.name*. The suffix, following the @ symbol, indicates the domain against which to authenticate the user.

If you are currently logged on to a system, pressing Ctrl+Alt+Delete takes you to the Windows 2000 Security dialog box, at which point you can do one of the following:

- Log off the system, which closes all programs and ends the instance of the shell.
- Lock the system, which allows programs to continue running but prevents access to the system. When a system is locked, you can unlock it by pressing Ctrl+Alt+Delete and entering the username and password of the user who locked the system or an administrator's username and password.



To lock a workstation automatically after a period of idle time, you use a screensaver password.

- ▶ Shut down the system.
- ▶ Change your password.
- ▶ Open Task Manager.

Automating Logon

You can configure Windows 2000 Professional systems so that you are not required to enter a username and password; in this case, your system automatically logs on as a specified user account. From the Users and Passwords applet in the Control Panel, you click the Advanced tab and clear the Require Users to Press Ctrl+Alt+Delete Before Logging On check box. The same setting is available through a group policy object (GPO) setting. GPOs are configured via Active Directory under Windows 2000 Server and Windows Server 2003; they are discussed later in this chapter.

Understanding Active Directory

Windows 2000's Active Directory goes far beyond what the Security Accounts Manager (SAM) database does for Windows NT 4. SAM and Active Directory both store security account information for users, groups, computers, and user rights, but that's where the similarity ends. Active Directory's database stores *objects* that represent enterprise resources, including users, groups, computers, printers, folders, applications, connections, security and configuration settings, and network topology. For each of these types, or *classes*, of objects, Active Directory can store numerous properties, or *attributes*. So a user account is far more than a username and password; it is information about the user's mailbox, the user's address and phone number, the role of the user within the organization (including the user's manager and location), and far, far more.

As a central store of information related to the enterprise network, Active Directory allows administrators to create a virtual representation or model of the enterprise—linking various objects together, grouping objects based on how they are administered, and structuring the enterprise information technology (IT) to best support the organization's goals. In addition, Active

Directory's database is *extensible*, which means you can customize and append it with additional attributes and object classes. So if an organization wants to keep track of salary information for each employee, it can simply extend the information that Active Directory stores about employees to include salary or, better yet, purchase a payroll application that is Active Directory aware and can automatically extend the directory appropriately.

A database is of no use if it simply stores information. One must be able to somehow access and manipulate that information in the database, and Active Directory includes numerous services, most based on Internet standard, that allow you to do just that. To provide the functionality required to search or query a database for a particular enterprise resource, locate that resource out on the network, manage that resource's record in Active Directory, and ensure that the record is consistent throughout the network.

Active Directory's database and services reside on servers that have been designated domain controllers. Unlike with Windows NT 4, Windows 2000 domain controllers are not created while the operating system is installed. Rather, a functioning server is *promoted* to act as a domain controller, at which time it obtains a copy of Active Directory and launches the required services. Also unlike with NT 4, there is no "primary" domain controller. All domain controllers can write to the directory. Therefore, a change to the domain is replicated to all domain controllers, making Active Directory a *multimaster* replication model.

For the Windows 2000 Professional exam, it is important that you have a basic understanding of Active Directory's structure, which, like that of Windows NT 4, begins with a domain. The *domain* is the fundamental administrative, security, and replication unit of Active Directory. The domain is specified by two names: its down-level Network Basic Input/Output System (NetBIOS) name—such as CONOSCO, which was also used in NT 4—and its DNS name, such as `conosco.com`. DNS is the primary name resolution methodology in Windows 2000.

When an enterprise decides to implement a multidomain model within its Active Directory database, it creates what are called domain *trees* or *forests*. Multidomain models, however, fall outside the scope of the Windows 2000 Professional exam, so this chapter focuses on what you need to know in a single-domain environment.

In a single domain, Active Directory can contain millions of objects. To increase the manageability of those objects, you can place them in containers called OUs. OUs can contain other OUs, allowing a nested, hierarchical structure to be created within a domain (see Figure 3.2).

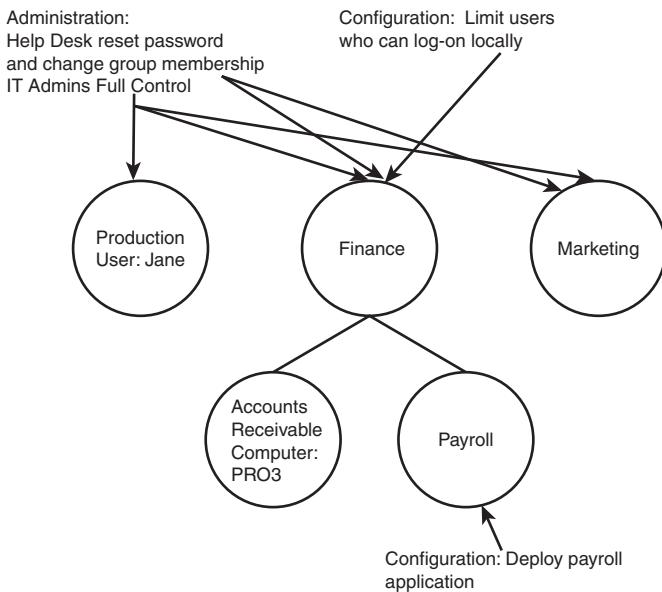


Figure 3.2 An example of an Active Directory domain that contains several OUs.

An enterprise uses its OU structure to control the administration and configuration of objects in the enterprise. For example, the organization depicted in Figure 3.2 might give an IT Admins group full control over the OUs displayed, which would allow that group to create, delete, and fully manage all the objects within those OUs. A Help Desk group might be given permission to reset passwords for user objects in the Finance and Marketing OUs and to put users in those OUs into groups based on the resource access they require. Workstations in the Finance OU could be configured to limit which users are allowed to log on locally. And users in the Payroll OU might have the payroll application installed on their machines, all through properties of the OU.

The OUs' virtual model of administration and configuration offers enormous flexibility and simplifies the effort it takes to manage large and small networks. As objects are moved between OUs, they are administered and configured differently. For example, referring to Figure 3.2, if a user named Jane is moved from the Production OU to the Payroll OU, the payroll application is deployed automatically. In addition, the Help Desk can reset Jane's password because, by default, properties of OUs (including delegated administrative permissions) are inherited from their parent OUs. If the computer PRO3 is moved from the Accounts Receivable OU to the Marketing OU, the limitation on which users can log on locally (which it was inheriting from the Finance OU) is removed.

The complexities and mechanics of designing and implementing Active Directory are not among the objectives of the Windows 2000 Professional exam. However, it is important that you realize that within a domain, you can use OUs to control administration and configuration of all objects, including users and computers, and that OUs by default inherit the administrative and configuration properties of OUs higher up in the OU structure. You will see these concepts in action in the section “Group Policy,” later in this chapter.

Understanding and Implementing Policy

Configuring a particular system and the environment for a particular user begins with its defaults—the settings determined by Microsoft during the development of Windows 2000. Of course, there are numerous settings for which Microsoft’s defaults are not appropriate for one or more computers or users. Therefore, users and administrators often find themselves modifying the defaults.

In the past, if several settings needed to be changed, you often had to use several tools, including User Manager, Server Manager, System Policy Editor, and even Registry Editor. If settings needed to be changed on multiple computers, it was often necessary to make those changes on each system individually. And if a setting you specified was later changed inappropriately, there was often no way to set it back to the desired setting except by manually making the change again.

Managing changes and configuration has been significantly improved in Windows 2000, thanks to the introduction into the Windows environment of *policy-based administration*. Policies provide administrators with a single list of configuration settings in one tool, rather than many tools, and allow administrators to apply those configuration settings to one machine, many machines, or every machine.

Local Policy

On a Windows 2000 Professional system, you can configure security-related settings by using the Local Security Settings console, which contains the Security Settings Microsoft Management Console (MMC) snap-in. To open this snap-in, you simply choose Start, Settings, Control Panel, Administrative Tools, Local Security Settings. Each of the nodes in the Local

Security Settings console is a security area or scope within which you will find dozens of security related settings (also called *attributes*).

The Local Setting column of the details pane displays the settings as specified by the local policy. The Effective Settings column shows what is currently in effect. The two columns may differ if the local policy has not been implemented; changes to security settings take effect when the system is restarted or following a refresh interval, which is by default 90 minutes. The columns may also differ because local policy settings are overridden by group policy settings, which is discussed later in this chapter.

Local policy settings include user rights assignments such as the ability of certain users to log on locally to the computer. You can use local policy to enable auditing for various types of events, such as which users are successfully or unsuccessfully logging on to the computer. You can use local policy to configure several different security options, such as whether to have Windows 2000 display the username of the last logged-on user in the Log On to Windows dialog box. Local policy also provides account policy settings for users that allow you to specify password requirements, among other things.

Account Policies

Account policies control the password requirements and how the system responds to invalid logon attempts. The policies you can specify include the following:

- *Maximum password age*—This is the period of time after which a password must be changed.
- *Minimum password length*—This is the number of characters in a password. Passwords can contain up to 127 characters; however, most passwords should not exceed 14.
- *Passwords must meet complexity requirements*—This policy, if in effect, does not allow a password change unless the new password contains at least three of four character types: uppercase (A through z), lowercase (a through z), numeric (0 through 9), and nonalphanumeric (such as !).
- *Enforce password history*—This policy specifies the number of previous passwords that the system can remember. When a user attempts to change his or her password, the new password is compared against the history; if the new password is unique, the change is allowed.
- *Minimum password age*—This specifies the number of days that a new password must be used before it can be changed again.

- *Account lockout threshold*—This is the number of denied logon attempts after which an account is locked out. For example, if this policy is set to three, a lockout occurs if a user enters the wrong password three times; any further logon attempts are denied. If this policy is set to zero, there is no lockout threshold.
- *Reset account lockout counter after*—This is the number of minutes after which the counter, which applies to the lockout threshold, is reset. For example, if the counter is reset after five minutes and the account lockout threshold is three, a user can log on twice with the incorrect password. After five minutes, the counter is reset, so the user can log on twice more. A third invalid logon during a five-minute period locks out the account.
- *Account lockout duration*—This specifies how long logon attempts are denied after a lockout. During this period, a logon with the locked out username is not authenticated.

Audit Policies

Audit policies specify what types of events are entered into the security log. The following are the most important policies to understand:

- *Logon events*—This policy deals with authentication of users logging on or off locally and making connections to the computer from remote systems.
- *Account management*—This policy deals with any change to account properties, including password changes and the addition, deletion, or modification of users or groups.
- *Object access*—This policy deals with access to objects on which auditing has been specified. Auditing object access, for example, enables auditing of files and folders on an NT File System (NTFS) volume, but you must also configure auditing on those files and folders. See Chapter 2, “Implementing and Administering Resources,” for a detailed discussion of auditing.
- *Privilege use*—This policy deals with use of any user right, called a *privilege*. For example, this policy audits a user who changes the system time because changing system time is a privilege.

For each policy, you can specify to audit successes, failures, or both. As events are logged, they appear in the security log, which can be viewed, by default, only by administrators. Other logs can be viewed by anyone.

User Rights Assignment

User rights, also called *privileges*, allow a user or group to perform system functions such as change the system time, back up or restore files, and format a disk volume. Some rights are assigned to built-in groups. For example, the Administrators group can format a disk volume. You cannot deny that right to members of the Administrators group, nor can you assign that right to a user or group you create. Other rights are assignable. For example, the right to back up files and folders is given by default to the Administrators group and the Backup Operators group, but you can remove the right for those groups or assign the right to other users or groups. You can modify the rights that are displayed in the Local Security Settings console. Other built-in rights that are not displayed in this console are not modifiable.

User rights, because they are system oriented, override object permissions when the two are in conflict with each other. For example, a user may be denied permission to read a folder on a disk volume. However, if the user has been given the privilege to back up files and folders, a backup of the folder succeeds, even though the user cannot actually read the folder.

Security Options

The Security Options node contains a number of useful security settings. This node highlights one of the advantages of using (local or group) policy settings: Although many of these settings are accessible elsewhere in the user interface (for example, you can specify driver signing in the System applet), policy settings allow you to compile all those settings, from all those tools and applets, into a unified configuration tool.

Some particularly useful options to be familiar with are the following:

- *Disable Ctrl+Alt+Delete requirement for logon*—If this policy is enabled, the logon dialog box does not appear at startup, and the system boots directly to the desktop. This policy is enabled by default on standalone systems and disabled by default when a machine joins a domain, due to the obvious security implications of bypassing a secure logon.
- *Clear the Virtual Memory Pagefile when the system shuts down*—With this policy, by default, the pagefile is not cleared and could allow unauthorized access to sensitive information that remains in the pagefile.
- *Do not display last username in logon screen*—This policy forces users to enter both usernames and passwords at logon. By default, this policy is disabled, which means the name of the previously logged-on user is displayed.

Managing Local Policies

The Local Security Settings console is most helpful on standalone systems. The local policy sets the configuration of the computer, and if a setting is changed through tools other than the Local Security Settings console, the change is reverted to the policy-specified setting when the system is restarted or following the policy refresh interval.

It is possible, however, to transfer security policies between systems. If you right-click the Security Settings node, you can export and import policies. This allows you to copy a policy you have created on one machine to other machines. However, you can imagine the complexity of trying to maintain consistent local policies across multiple systems. That complexity is addressed by group policy, which is discussed in the following section.



The Security Configuration and Analysis snap-in allows you to capture the security configuration of a system as a database and to use that database as a baseline against which you can gauge changes to security settings. When modifications are made that deviate from the database setting, you can reapply the original setting. You can also save the database as a template, which you can then apply to other systems to duplicate security settings. There are also preconfigured security templates that you can apply to Windows 2000 systems to implement a variety of security environments.

Group Policy

Group policy (technically referred to as GPOs) applies the concept of policy-enforced configuration to one or more computers with one or more users. Similar to local policy, group policy provides Active Directory administrators with a centralized group of configuration settings that get inherited from a parent container, such as a domain, to child containers, such as OUs, that are stored within the domain. You can apply, or *link*, a group policy to the following:

- *A domain*—This causes the configuration specified by the policy to be applied to every user or computer within the domain.
- *An OU*—This applies group policy settings to users or computers within the OU.
- *A site*—This is an Active Directory object that represents a portion of your network topology with good connectivity (such as a local area network [LAN]).

To access group policy, you must go to the properties of a site, domain, or OU (SDOU) and click the Group Policy tab. Therefore, to work with group policy for a site, you use the Active Directory Sites and Services console, right-click on a site, and choose Properties. To work with group policy for a

domain or an OU, you use the Active Directory Users and Computers console, right-click a domain or an OU, and choose Properties.

Whereas an individual machine can have only one local policy, an SDOU can have multiple policies. On the Group Policy properties sheet, you can create a new GPO by clicking New or you can link an existing group policy to the SDOU by clicking Add. If you select a group policy and click Edit, you expose the GPO in the Group Policy Editor.



NOTE

The terms *group policy* and *GPOs* are routinely used interchangeably. Whenever you hear or see references made to group policy in relation to Active Directory, rest assured that, technically, GPOs are being discussed.

Application of Group Policy

Group policy (or GPOs) are divided into the Computer Settings and User Settings nodes. The computer settings apply to every computer in the SDOU to which the policy is linked and, by default, to all child OUs. Computer settings take effect at startup and every refresh interval (which is by default 90 minutes). User settings affect every user in the SDOU and its children at logon, and after each refresh interval.

When a computer starts up, its current settings are modified first by any configuration specified by the local policy. Then, the configuration in group policies is applied: first, the policies linked to the computer's site, then the policies for its domain, and finally the policies for each OU in the branch that leads to the computer's OU. If there is ever a conflict in a particular configuration setting, the last setting applied takes effect. Therefore, the policies that are "closest" to the computer—for example, the policies linked to its OU—take precedence if a conflict arises. The same application of policies applies to a user at logon: local policy, site policy, domain policy, and OU policy.



You can remember the order of policy application as LSDOU, or "el-stew." Policies are applied in the order local, site, domain, and OU.

The process of applying group policy settings is an intuitive process, at first. But applying group policy can get extremely complex when multiple policy settings are applied to a single container (SDOU), when inheritance is blocked or No Override is specified, and when policies are modified by

access control lists (ACLs). Luckily, the enterprise scale application of group policy is not an objective of the Windows 2000 Professional exam. You need to simply understand the basic order of policy application—local, site, domain, and OU (LSDOU).

Group Policy and OU Design

Group policy is a major factor in determining an enterprise's OU structure. If an OU contains users or computers that require different configurations and settings, the best practice is to create separate OUs, each of which contains objects that are configured similarly. By doing so, you can then manage the configuration by applying an appropriate group policy to each OU.

For example, think about the organization depicted in Figure 3.2. If within the Marketing OU a group of salespeople needed a sales application, and that sales application was not appropriate for all users in the Marketing OU, the best practice would be to create an OU, perhaps called Sales, within the Marketing OU (see Figure 3.3). If you place the Sales OU within the Marketing OU, the Sales OU inherits all the existing administration and configuration of the Marketing OU. But you can create a policy linked only to the Sales OU, and you can use that policy to deploy the sales application. As users are moved into the Sales OU, the sales application is deployed to them. See Chapter 4, “Configuring and Troubleshooting the User Experience,” for more information about deploying applications through group policy.

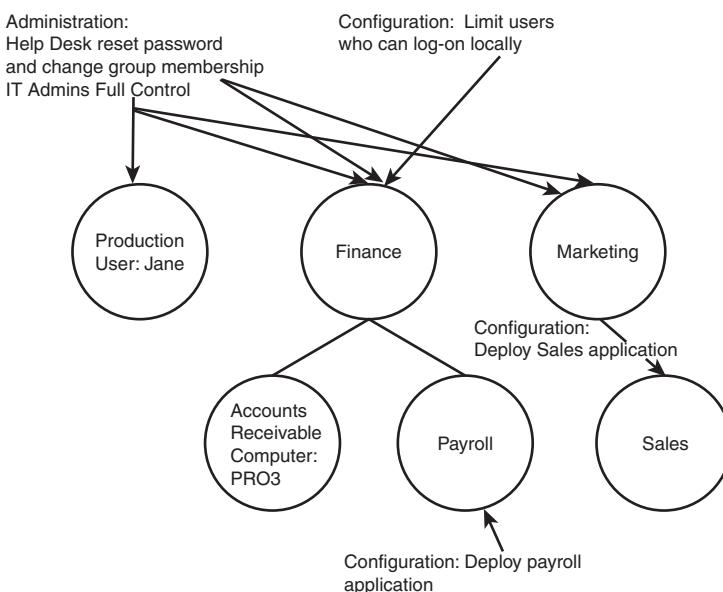


Figure 3.3 The Sales OU within the Marketing OU.

Practice Questions

Question 1

Computer1 is a member of the SAFTA domain. A local user account, **John**, is in the Administrators group. When John logs on to the SAFTA domain, he is unable to perform all administrative functions on his system. What should you do to enable John to have full administrative control over his computer?

- a. Delete the local user account **John**.
- b. Add John's domain user account to the Administrators group.
- c. Add John's domain user account to the Administrators group on the domain.
- d. Give John Full Control permission to the **C:\WINNT** directory.

Answer B is correct. John is logging on to the domain, and even if his domain username is **John**, it is still a different account than the local user account. Therefore, John is not actually a member of the Administrators group when he is logging on to the domain.

Question 2

Susan is an administrator of **Computer5**. Other users who log on to **Computer5** complain that Susan occasionally formats the **D:** drive to get rid of old files and folders and that she is destroying their data in the process. You want Susan to be able to manage basic user and group accounts as well as restore files, but you want to prevent her from unnecessarily harming the system. What should you do? (Select all the correct answers.)

- a. Add Susan to the Backup Operators group.
- b. Add Susan to the Power Users group.
- c. Deny Susan Full Control permission to the **System32** folder.
- d. Remove Susan from the Administrators group.

Answers a, b, and d are correct. The Backup Operators group can restore files and folders, and the Power Users group can manage basic user and group accounts. By removing Susan from the Administrators group, you deny her many privileges that are built in to that group, including the privilege to format disk volumes.

Question 3

You want to enable a colleague to access files on your Windows 2000 Professional system from her system, which is part of a Novell network. You have shared the folder in which the files are stored, and both share and NTFS permissions indicate that Everyone has Full Control. However, your colleague calls you and indicates that she still cannot access the files. What can you do to grant her access? (Select all the correct answers.)

- a. Give the Authenticated Users group Full Control of the folder.
- b. Create a user account for your colleague and tell her the password.
- c. Enable the Guest account and tell your colleague the password.
- d. Stop the **WINLOGON** service.

Answers b and c are correct. In order to access a resource, one must first have a valid user account. Because the system is part of a Novell network, it is not in a domain and is a standalone or workgroup system. Therefore, all accounts must be created locally. You can either create an account for your colleague or enable the Guest account.

Question 4

You have just installed Windows 2000 Professional, and when it starts up, it goes directly to the desktop, without asking for a username and password. You want to improve the security of the system by enforcing logon. What tools could you use? (Select all the correct answers.)

- a. Local security policy
- b. Domain security policy
- c. Group policy
- d. The Users and Passwords applet
- e. The System applet
- f. The Computer Management console

Answers a, c, and d are correct. All three of these tools expose the security setting to automate logon or require logon. The System applet and the Computer Management console do not expose the setting to require logon. Therefore, Answers e and f are incorrect.

Question 5

You are deploying a mobile computer called **Laptop3** for Maria. **Laptop3** is in the Sales OU. Maria is in the Outside Sales OU, which is contained within the Sales OU. You want to ensure that the sales application is deployed to Maria and all others who take **Laptop3** on the road. Which of the following is the best-practice solution for deploying the sales application?

- a. Configure the User Settings node of a GPO to deploy the application's Windows Installer Package (MSI) file to the Outside Sales OU.
- b. Use local policy to deploy the application's MSI file to **Laptop3**.
- c. Configure the User Settings node of a GPO to deploy the application's MSI file to the Sales OU.
- d. Configure the Computer Settings node of a GPO to deploy the application's MSI file to the Outside Sales OU.
- e. Configure the Computer Settings node of a GPO to deploy the application's MSI file to the Sales OU.

Answer e is correct. You want all users to have the application when they are on **Laptop3**, so you want to use the Computer Settings node of group policy. **Laptop3** belongs to the Sales OU. Applying the policy to the Outside Sales OU would not affect **Laptop3**, which is above the Outside Sales OU in the OU structure.

Question 6

Lou has an account in the domain that is a member of the Sales, Trainers, and Managers groups. You are hiring Beth, who will be a member of the same groups as Lou. You want to create Beth's account with the least administrative effort. What should you do?

- a. Create an account for Beth and add the account to the Sales, Trainers, and Managers groups.
- b. Rename Lou's account as Beth.
- c. Copy Lou's account and call the new account Beth.
- d. Rename the Guest account Beth.

Answer c is correct. If you copy Lou's account, the new account will be a member of the same groups as Lou's.

Question 7

Lou has a local user account that is a member of the Sales, Trainers, and Managers groups. You are hiring Beth, who will also be a member of the same groups. You want to create Beth's account with the least administrative effort. What should you do?

- a. Create an account for Beth and add the account to the Sales, Trainers, and Managers groups.
- b. Rename Lou's account as Beth.
- c. Copy Lou's account and call the new account Beth.
- d. Rename the Guest account Beth.

Answer a is correct. You cannot copy a local user account.

Question 8

Lou has an account in the domain that is a member of the Sales, Trainers, and Managers groups. The Sales group has access to the Sales Reports folder, the Trainers group can read the Curricula folder, and the Managers can read the Financials folder. Lou can also modify the Curricula folder. You hire Beth, who will be performing the same job function as Lou. You copy Lou's account and name the new account **Beth**. Which of the following statements are true? (Select all the correct answers.)

- a. Beth is a member of the Sales, Trainers, and Managers groups.
- b. Beth can read the Curricula folder.
- c. Beth can modify the Curricula folder.
- d. Beth's password is the same as Lou's.

Answers a and b are correct. The access Beth enjoys is because her account is a member of the same groups as Lou's, but access permissions assigned to a user account are not changed when you copy the account. Similarly, user passwords are not copied when an account is copied. Beth cannot modify the Curricula folder because that permission was assigned directly to Lou. Therefore, Answer c is incorrect.

Question 9

You bring your system from your home network into the office and connect it to the enterprise network. When you log on, the settings and applications that normally affect you at the office do not apply. What can you do to correct the situation?

- a. Renew your system's DHCP address.
- b. Log on with the Administrator account.
- c. Join your system to the domain and log on with your domain account.
- d. Log on as with the Guest account.

Answer c is correct. The system is not part of the domain, so it does not apply policies that are part of your domain's Active Directory database.

Question 10

You have configured the local policy of your domain workstation, a Windows 2000 Professional machine, to disable the requirement to press Ctrl+Alt+Delete and log on. However, when you start the computer, it still requires you to press Ctrl+Alt+Delete. What tool should you use to locate the source of the problem?

- a. Computer Management
- b. System Information
- c. Event Viewer
- d. Local security policy
- e. Group policy

Answer e is correct. Your system's local policy is being overridden by a site, a domain, or an OU group policy. Group policy allows you to examine the policies applied to your system's SDOUs. Although local security policy shows you that there is a discrepancy between the local policy and the effective policy, it does not help you locate the source of the discrepancy. Therefore, Answer d is incorrect.

Need to Know More?



Microsoft Corporation. *Microsoft Windows 2000 Professional Resource Kit*. Redmond, Washington: Microsoft Press, 2000. This book has invaluable information on implementing security accounts and policy.



Stinson, Craig, and Carl Siechert. *Running Microsoft Windows 2000 Professional*. Redmond, Washington: Microsoft Press, 2000. This guidebook to Windows 2000 Professional is a good source for information on user and group account management.



Hudson, James, and Fullerton, Sean. *Special Edition Using Microsoft Active Directory*. (ISBN: 0789724340), Indianapolis. Que Publishing, 2001. This book provides complete, in-depth coverage of the newest directory service from Microsoft. Authors Fullerton and Hudson use their previous training and administration experiences to explain how to design, implement, and troubleshoot using Active Directory.



To find more information, you can search the TechNet CD (or its online version, through www.microsoft.com) and/or the Windows 2000 Professional Resource Kit CD using the keywords account, policy, SAM, authentication, group, user rights, and group policy.

